

# Investigation & Prosecution of Cybercrime: Introduction

## CJ341 – Cyberlaw & Cybercrime Lecture #16

M. E. Kabay, PhD, CISSP-ISSMP  
<mailto:mikabay@norwich.edu>  
 V: 802.479.7937  
 Program Director, MSIA,  
 School of Graduate Studies

P. R. Stephenson, PhD, CISM, CISSP, FICAF  
<mailto:pstephen@norwich.edu>  
 V: 802.498.4923  
 Associate Program Director, MSIA  
 School of Graduate Studies  
 Chair, Department of Computing  
 School of Business & Management

Julie Tower-Pierce, Esq  
<mailto:j@hjit.net>  
 Adjunct Prof Justice Studies  
 School of Social Sciences

1

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Topics

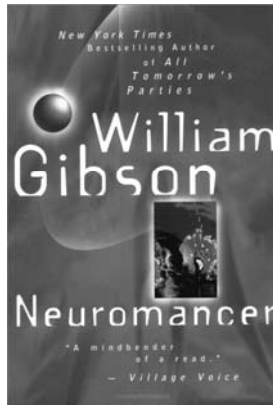
- Overview of Cyberspace
- Moore
  - ❑ Tracing a Suspect on the Internet
  - ❑ Locating Information from E-Mails
  - ❑ Proactive vs Reactive Strategies
- Clifford
  - ❑ Three Cybercrime Scenarios

2

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Overview of Cyberspace

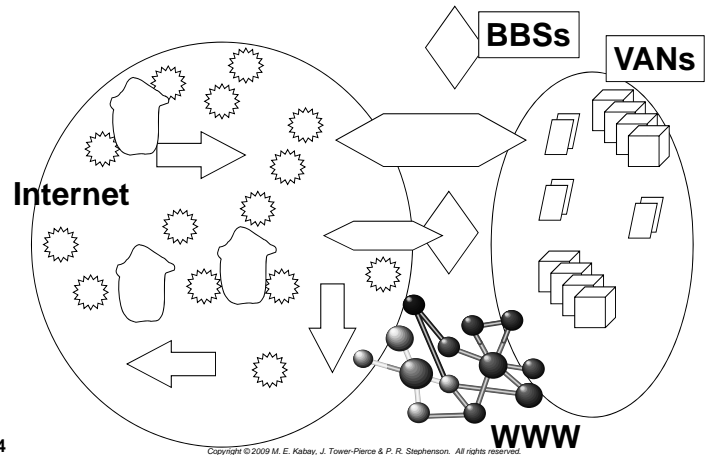
- The Evolution of Cyberspace
- News
- The Internet
- The World Wide Web



3

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

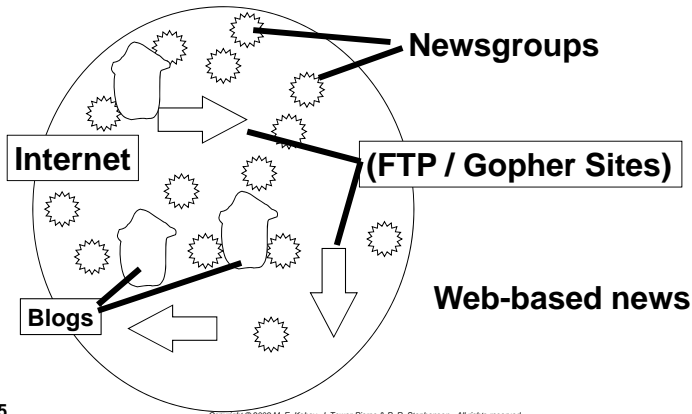
## Evolution of Cyberspace



4

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

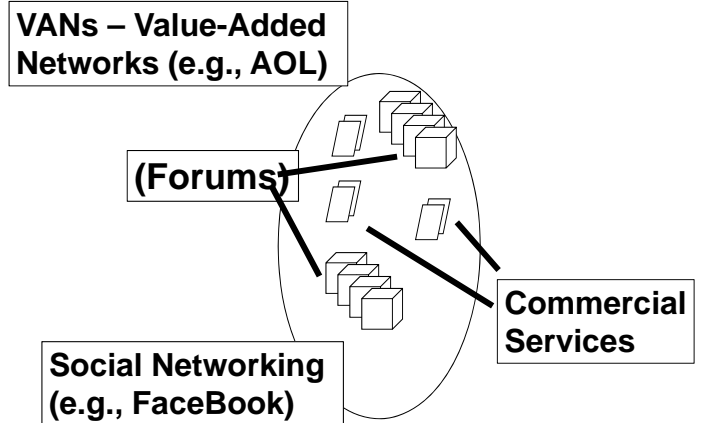
## Disintermediated News



5

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

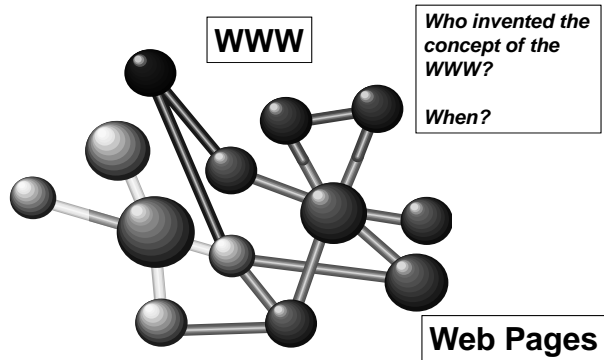
## Discussions



6

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## The Web



7

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Online Forums

- Types
  - Usenet
  - IRC
  - ICQ
  - Mailing lists
  - Private or public discussion groups
    - ✓ Yahoo Groups
    - ✓ GOOGLE Groups
- Chat Clients often include multi-user capabilities
  - AIM, Trillian, Digsby....

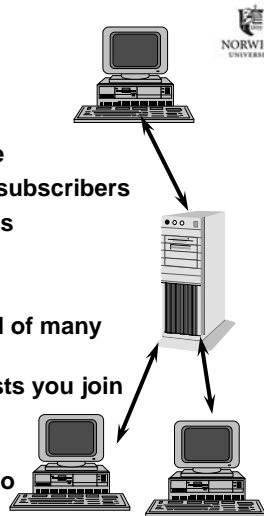
*These communications channels may be critically important in forensic investigations; e.g., CISO at NU regularly uses these channels when investigating alleged security or honor-code violations.*

8

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Online Forums & Mailing Lists

- Mailing-list software
  - Users subscribe & unsubscribe
  - Sends out e-mail messages to subscribers
  - Copies replies to all participants
  - e.g., Majordomo
- Some mailing lists have Digests
  - Single large file per day instead of many messages
  - Check the options in mailing lists you join
- Online special-interest portals include discussions
  - E.g., commentary in response to postings



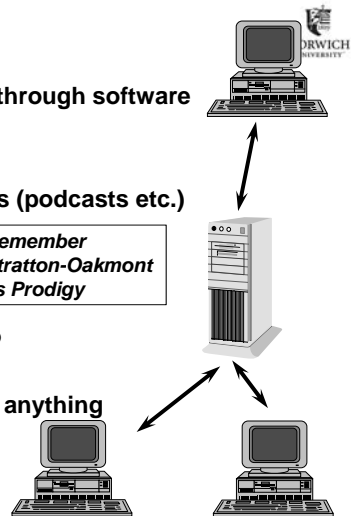
9

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Online News

- Users access news groups through software
  - E.g., USENET (NEWS://)
  - Other groups, blogs
  - RSS feeds from Web sites (podcasts etc.)
- Moderated newsgroups
  - Editor/moderator
  - Controls what appears
  - High signal-to-noise ratio
- Unmoderated
  - Automatic distribution of anything
  - Low signal-to-noise ratio
  - Subject to *spamming*

*Remember Stratton-Oakmont vs Prodigy*



10

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Online Forums: BBSs (OLD)

Historical interest (e.g., *War Games*, 1983)

- Access via phone calls & modems
- Professional and amateur
- May require long-distance calls
- Unregulated: hatred, obscenity
- Some moderated, others unmoderated
- Unreliable: virus-infected software
- A few run by and for criminals
  - Stolen software
  - Ads for stolen goods

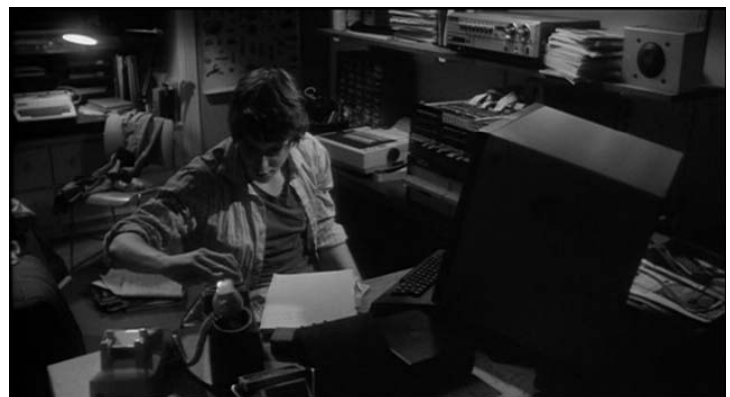


11

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## War Games (1983)

- IMDB: <http://www.imdb.com/title/tt0086567/>



# The Internet

- An internet is network of networks
  - ❑ The Internet grew out of ARPANET
  - ❑ Based on TCP/IP linkage of networks (see next slide)
- Includes > 1B users
  - ❑ Has 200-300 million nodes
  - ❑ Growing by 2,000,000 users/month
- Users often have free (uncharged) access
  - ❑ Some cities have "Freenet" service

# The Internet

- TCP/IP based internetworking
  - ❑ Transmission Control Protocol = TCP
  - ❑ Internet Protocol = IP
  - ❑ Packet-switched protocols
  - ❑ Dynamic routing of packets for high efficiency
- Began as DARPA project in late 1960s
  - ❑ Defense Advanced Research Projects Agency
  - ❑ Steady expansion during 1970s & 1980s
  - ❑ Explosive growth late 1980s and in 1990s
  - ❑ .com domain opened for general use in 1993

# Recent Internet Usage Stats

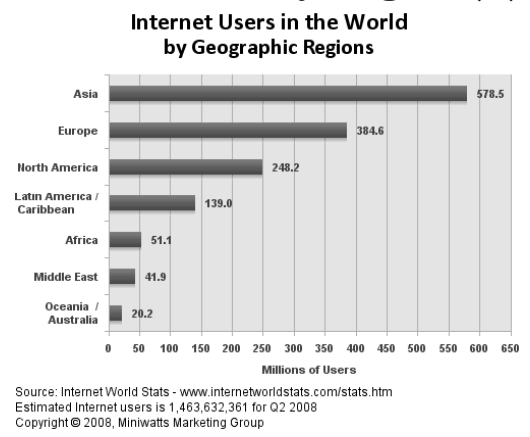
http://www.internetworldstats.com/stats.htm

### INTERNET USAGE STATISTICS The Internet Big Picture World Internet Users and Population Stats

World Regions	Population (2008 Est.)	Internet Users Dec/31, 2008	Internet Usage, Latest Data	% Population (Penetration)	Usage % of World	Usage Growth 2000-2008
Africa	955,206,348	4,514,400	51,065,630	5.3 %	3.5 %	1,031.2 %
Asia	3,776,181,949	114,304,000	578,538,257	15.3 %	39.5 %	406.1 %
Europe	800,401,065	105,096,093	384,633,765	48.1 %	26.3 %	266.0 %
Middle East	197,090,443	3,284,800	41,939,200	21.3 %	2.9 %	1,176.8 %
North America	337,167,248	108,096,800	248,241,969	73.6 %	17.0 %	129.6 %
Latin America/Caribbean	576,091,673	18,068,919	139,009,209	24.1 %	9.5 %	669.3 %
Oceania / Australia	33,981,562	7,620,480	20,204,331	59.5 %	1.4 %	165.1 %
WORLD TOTAL	6,676,120,288	360,985,492	1,463,632,361	21.9 %	100.0 %	305.5 %

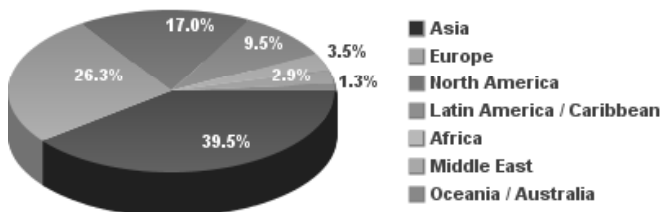
NOTES: (1) Internet Usage and World Population Statistics are for June 30, 2008. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau. (4) Internet usage information comes from data published by Netstat/NetRating, by the International Telecommunications Union, by local NIC, and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surling Guide, now in ten languages. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 - 2008, Miniwatts Marketing Group. All rights reserved worldwide.

# Internet Users by Region (1)



# Internet Users by Region (2)

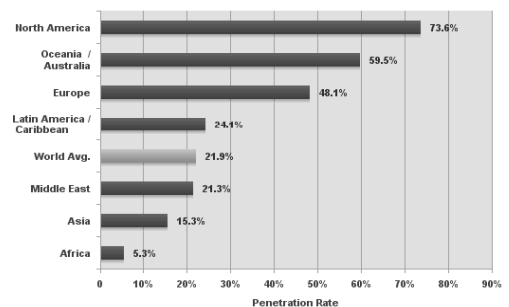
## World Internet Users by World Regions



Source: Internet World Stats - www.internetworldstats.com/stats.htm  
1,463,632,361 Internet users for June 30, 2008  
Copyright © 2008, Miniwatts Marketing Group

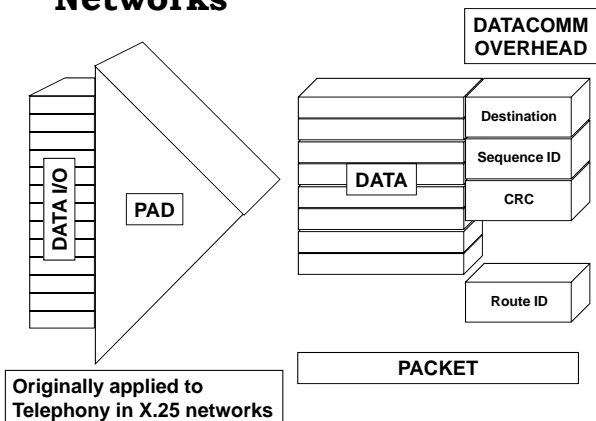
# Internet Penetration Rates by Region

## World Internet Penetration Rates by Geographic Regions



Source: Internet World Stats - www.internetworldstats.com/stats.htm  
Penetration Rates are based on a world population of 6,676,120,288 for mid-year 2008 and 1,463,632,361 estimated internet users.  
Copyright © 2008, Miniwatts Marketing Group

## Basics: Packet-Switching Networks

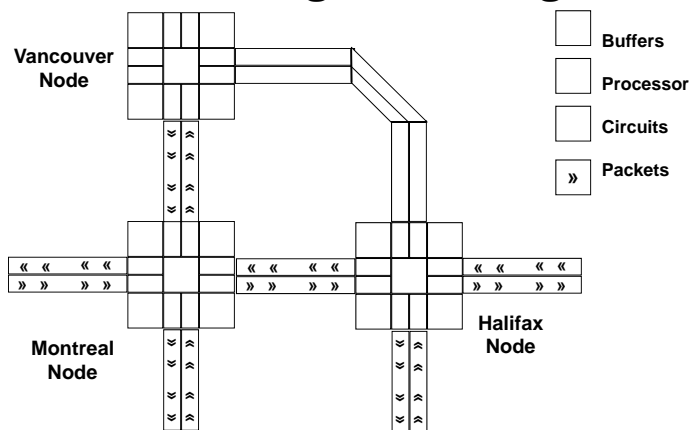


Originally applied to Telephony in X.25 networks

19

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

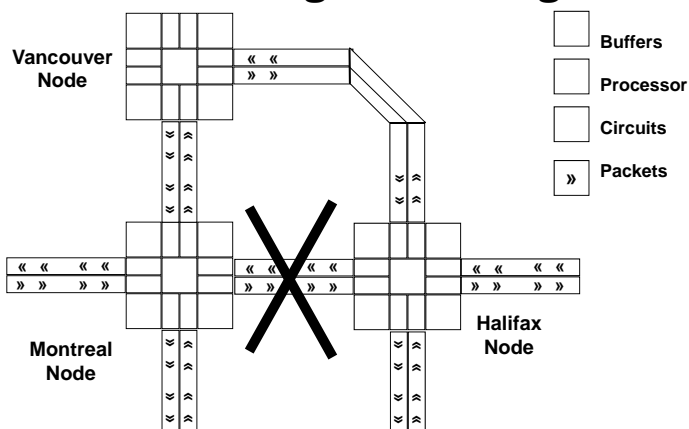
## Basics: Datagram Routing



20

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Basics: Datagram Routing



21

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Basics of TCP/IP -- Video

➤ *Warriors of the Net*: 12 minutes – used by permission of the authors.

[http://www.mekabay.com/overview/warriors\\_of\\_the\\_internet.mpg](http://www.mekabay.com/overview/warriors_of_the_internet.mpg)



22

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Tracing a Suspect on the Internet

- The Dynamic IP Address
- Locating the Host
- DNS Lookup
- betterwhois.com
- SamSpade Program
- Locating Information from E-Mails
- E-Mail Headers

23

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## The Dynamic IP Address

- Suspect may have own connection to 'Net'
  - Has permanent IP address
  - E.g., gmail.com has IP address 64.233.171.83
  - Norwich.edu is 192.149.109.197
- Or suspect connects to Internet via ISP
  - DHCP (Dynamic Host Configuration Protocol)
  - User is assigned temporary "dynamic" address
  - Re-used and not unique
  - Logged by ISP for some time (days to forever)
  - Must absolutely get cooperation of ISP and obtain records (if they still exist) under subpoena
  - The records will show match of dynamic address to user's modem's MAC (media access control) address and from there to the assigned modem location, authorized user, address and so on

What would an unsecured WAP do to this linkage?

24

Copyright © 2009 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

## Locating the Host

- ICANN (Internet Corporation for Assigned Names and Numbers) <http://www.icann.org/>
  - ❑ Global coordination of IP address assignments
  - ❑ Defines rules for domain names
- InterNIC < <http://www.icann.org/> > points to registrars around world
  - ❑ See lists e.g., <http://www.internic.net/origin.html>
  - ❑ Australia has 13 registrars
  - ❑ Canada has 152
  - ❑ US has 562

## DNS Lookup

- WHOIS functions available online from each registrar
  - ❑ But <http://www.betterwhois.com/> works with all registrars (see next page)
- Many other tools available online for DNS lookup
- SamSpade tool and service from <http://www.samspade.org> can find many records as well as providing additional functions (see page after next)
- Info in registry may be false or out of date
  - ❑ Often see dummy phone numbers in DNS



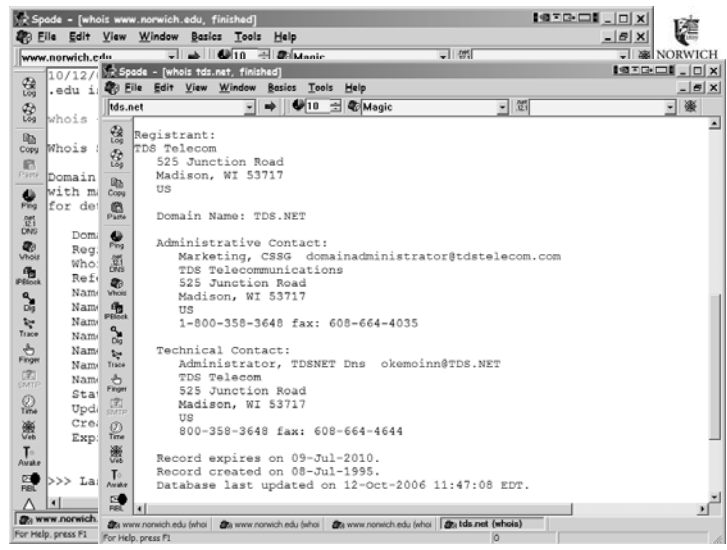
### What's wrong with WHOIS?

The domain business has been deregulated... For the first time, many different domain registrars are granting domain names.

But there is a problem, the standard WHOIS domain search used on thousands of web sites is no longer accurate. Why? Because each domain registrar now keeps their own WHOIS database which doesn't include domains registered by competing registrars.

WWW.

Searches shared database registry and queries appropriate registrar.



## Locating Information from E-Mails

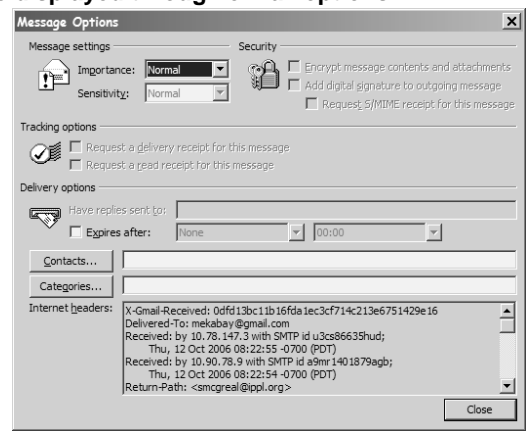
- Headers are crucially important
  - ❑ Often stripped from display



## E-Mail Headers

- Can be displayed through e-mail options

This example is from MS-Outlook



## E-Mail Headers

➤ Show details of who sent e-mail and how it was routed  
 X-Gmail-Received: 0dfd13bc11b16fdalec3cf714c213e6751429e16  
 Delivered-To: mekabay@gmail.com  
 Received: by 10.78.147.3 with SMTP id u3cs86635hud;  
 Thu, 12 Oct 2006 08:22:55 -0700 (PDT)  
 Return-Path: <smcgreal@ippl.org>  
 Received: from mail42.opentransfer.com (mail42.opentransfer.com [71.18.111.198])  
 by mx.google.com with SMTP id 29s1861796wr1.2006.10.12.08.22.53;  
 Thu, 12 Oct 2006 08:22:54 -0700 (PDT)  
 Received-SPF: neutral (google.com: 71.18.111.198 is neither permitted nor denied by best guess record for domain of smcgreal@ippl.org)  
 Received: (gmail 11919 invoked by uid 399); 12 Oct 2006 14:54:05 -0000  
 Received: from unknown (HELO System5.ippl.org) (70.60.217.92)  
 by mail42.opentransfer.com with SMTP; 12 Oct 2006 14:54:05 -0000  
 Message-Id: <7.0.1.0.2.20061012104204.03aldaf8@ippl.org>  
 X-Mailer: QUALCOMM Windows Eudora Version 7.0.1.0  
 Date: Thu, 12 Oct 2006 10:54:04 -0400  
 To: <mekabay@gmail.com>  
 From: Shirley McGreal <smcgreal@ippl.org>  
 Subject: Re: Orangutans  
 In-Reply-To: <200610121353.k9CDr1N3004352@cronus.email.starband.net>

NEVER simply forward an e-mail of interest to an investigator; always copy and paste the headers into your message to avoid corrupting the header.

31

## Proactive vs Reactive Strategies

- Some crimes are difficult to locate before they happen – need victim complaint to find out
  - Identity theft
  - Cyberstalking
- Others benefit from dragnets
  - Child pornography
  - Child abuse
- Officers need familiarity with argot (slang), culture

32

## Online Stings: Entrapment?

- Must not give any basis for claim that officer *initiated, suggested, prompted, or encouraged*
  - Illegal activity or
  - Investigative actions that violate privacy or
  - Convert a civilian into an agent of law enforcement to violate legal restrictions
- ENTRAPMENT can destroy case
  - Why? 4<sup>th</sup> Amendment safeguards
- Sorrells v. United States (1932)
  - SCOTUS ruled that entrapment defense must show proof that LEO *encouraged* crime
  - Defendant *would not have been predisposed* to commit crime

33

## United States v. Poehlman (2000)

- Poehlman alleged to have met undercover LEO to have sex with minor
- But defendant said he started online discussions with LEO to form *adult* relationship
- LEO wrote she was looking for someone “to train her daughters in the ways of the world”
- Poehlman explicitly said he wasn’t interested and LEO responded that she would terminate relationship
- Poehlman offered to “train” daughters as way of continuing relation but claimed he had no intention of having sex with them – was ploy
- SCOTUS ruled in favor of defendant: evidence that pedophilia was not his original intent & LEO was significantly responsible for his actions

34

## Three Cybercrime Scenarios

**YOU ARE RESPONSIBLE FOR STUDYING THESE CASES IN DETAIL**

- Cases presented by Ivan Orton in Ch 3 of Prof Clifford’s text:
  - Janet Davis – intrusion and data theft
  - Mel Howard – intrusion and data destruction
  - Allen Worley – harassment and stalking via e-mail
- Study closely – will be discussed throughout remainder of course AND IN EXAMS
  - Events
  - Investigation
  - Prosecution

35

# DISCUSSION

36